Estudio Sobre el Estado Del Arte de la Seguridad Informática en el Ecuador y sus Necesidades Reales

Luis Solórzano Cadena [(1)] Jenny Rezabala Triviño [(2)] Ing. Alfonso Aranda [(3)]
Facultad de Ingeniería Eléctrica y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 vía Perimetral
Apartado 09-01-5863. Guayaquil-Ecuador
zolorsano@gmail.com[(1)] jrezabala@gmail.com[(2)]
Escuela Superior Politécnica del Litoral, Ecuador, 2002, Ingeniero en Computación [(3)]
aaranda@telconet.ec, 2009 profesor de la ESPOL [(3)]

Resumen

Actualmente los sistemas informáticos son parte de nuestras vidas directa o indirectamente, de nuestra economía, y de la manera de cómo vivimos, ante este fenómeno la información se ha convertido en el activo más valioso, la misma que es necesario protegerla de las incontables amenazas que hay y se generan a cada momento, aquí es donde intervienen los sistemas de seguridad informática, los cuales deben ser lo suficientemente sofisticados y estar lo suficientemente preparados para contrarrestar y garantizar la disponibilidad, confidencialidad e integridad de la información, en este proyecto hemos obtenido de manera cuantitativa resultado muy interesantes con respecto al Estado del Arte de la Seguridad Informática en el Ecuador, el cual indica cual es la aptitud de las empresas ecuatorianas ante la seguridad informática, los actuales mecanismos y sistemas de protección que están adoptando, y cuáles son los dispositivos de protección mayormente utilizados, además con estos resultados se han podido determinar las oportunidades de negocios y emprendimientos que existen en nuestros mercado con respecto a la seguridad informática.

Palabras Claves: *Seguridad Informática, amenazas, Estado del Arte, disponibilidad, confidencialidad, integridad.*

Abstract

Currently computer systems are part of our lives directly or not, in our economy, and it defines basically our way of life, this makes them that the information be the most valuable asset, at the same time, we are oblige to protect them from the threats that are continuously present that keep evolving and improving, this when the information security systems have to be sufficiently sophisticated and constantly updated to counteract and guarantee the confidentiality, integrity and availability of the information, in this project we have a quantitative research with very interesting results about of the state of the art of Ecuadorian information security systems, this tell us, what is the aptitude of Ecuadorian enterprises about information security systems, the current mechanism and protection systems that they are implementing, and tell which ones are the devices of protection that are majorly used, and also with the current results it has been capable to determinate business opportunities and entrepreneurship that are currently in our market regarding security systems.

Keywords*: Information, security, threats, State of the art, availability, confidentiality, integrity.*

1. Introducción

Hoy en día la seguridad informativa se ha convertido a nivel global en el punto fuerte a preservar y mantener, las amenazas están solo esperando la mínima vulnerabilidad para penetrar en los sistemas de información y sacar la mayor cantidad de información posible, la misma que al final de alguna u otra manera produce ganancias económicas en manos de quien la sustrajo.

El internet nos ha unido en un solo mundo, donde cada milisegundo compartimos información de diversas índoles, esto hace que sin importan el status social o del nivel de desarrollo del país podamos tener acceso a los últimos avances tecnológicos, absorber información solo bajo nuestra propia responsabilidad, así como gozar de todos los beneficios que nos ofrecen las aplicaciones, pero también podemos ser víctimas del cibercrimen y comprometer nuestros intereses y el de los demás, si no tomamos las debidas medidas de seguridad.

Actualmente los países empezando por los de mayor desarrollo están preocupados en conocer cuál es el nivel de seguridad que poseen a nivel de nación ante las amenazas del ciberespacio, en el Ecuador preocupados por conocer nuestro nivel de seguridad hemos realizado el estudio del estado del arte de la seguridad informática, el cual nos da una idea cuantitativa de cuál es el nivel más alto de seguridad informática actualmente.

2. Objetivos.

El objetivo de esta investigación es definir el estado del arte de la seguridad informática en el Ecuador, identificar el nivel de aceptación por mercados de los servicios de gestión de seguridad e identificar oportunidades de emprendimiento.

3. Técnica de evaluación.

Para realizar el estudio de manera cuantitativa se selecciono como técnica de evaluación, a la encuesta, en base a que mediante la misma se obtiene datos de diferentes personas (empresas) respecto a un tema, situación o problema; describiendo el funcionamiento que permita comparar situaciones anteriores y las condiciones existentes en el desarrollo de la situación evaluada. La información que se obtiene es un recurso valioso y aplicable a sectores magnos del universo; del cual se obtienen importantes opiniones.

3.1 Calculo del tamaño de la muestra.

Para el cálculo de la muestra utilizaremos la siguiente formula estadística que está condicionada por el nivel de confianza, probabilidad de éxito, fracaso y máximo error permisible.

$$n = \frac{z^2 (p * q)}{e^2}$$

n: Tamaño de la muestra.
Z: Porcentaje de datos que se alcanza dado un porcentaje de confianza del 92%.
p: Probabilidad de éxito.
q: Probabilidad de fracaso.
e: Máximo error permisible

Considerando a p y q como 0,5 y trabajando con el valor de Z correspondiente para este caso, se obtiene.

$$n = \frac{(1.75)^2 (0.5 * 0.5)}{(0.08)^2}$$

$$n = 119.62$$

Por ende se trabajo con una muestra de 120, la cual fue tomada en el año 2011.

4. Análisis de resultados

4.1 El mercado Ecuatoriano.

Para este análisis hemos clasificado al mercado ecuatoriano en tres grupos, Home, Pymes y corporativos, de antemano conociendo que existe una diferencia considerable entre el Home y Pymes no así entre Pymes y Corporativos, se decidió hacer el análisis de la encuesta en dos grupos, Home y Empresariales, los cuales tendrán encuestas separadas y con la misma muestra de 120.

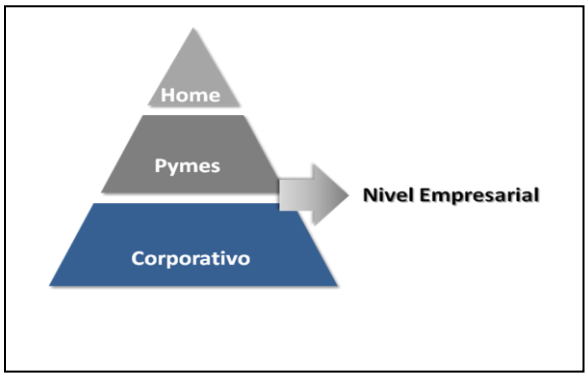

Figura 1. El mercado ecuatoriano.

4.2 Análisis de resultados del segmento Home

Para el resultado obtenido a nivel de home, mencionares solo los más relevantes para este informe, ya que se le dará un mayor enfoque al mercado empresarial corporativo.

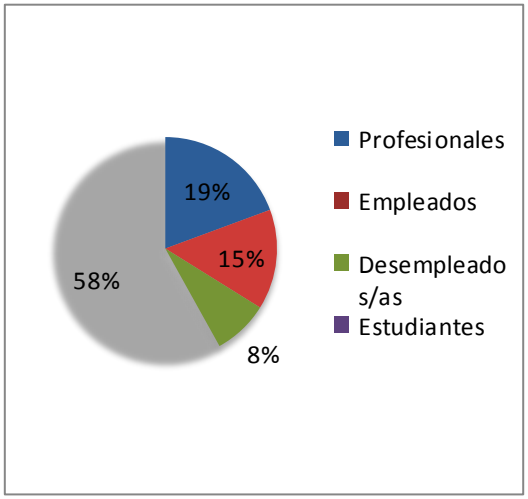

Figura 2. Ocupación de los encuestados

En la grafica podemos notar que a nivel de Home, la mayor parte de la encuesta ha sido hecha a estudiantes.

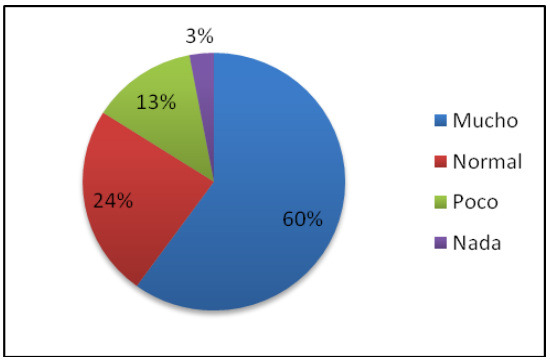

Figura 3. Impacto de la seguridad informática en el mercado laboral.

A pesar de ser estudiantes, hay un alto desconocimiento sobre la seguridad informática en el mercado laboral.

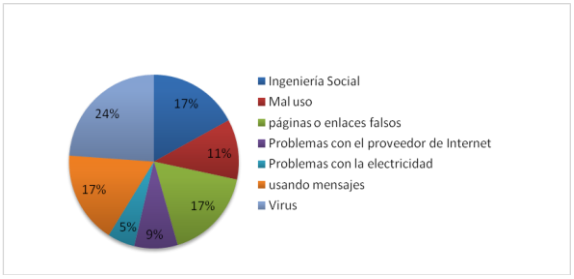

Figura 4. Métodos que la gente conoce, de cómo pueden ser atacados por una amenaza

Por otro lado es alentador saber que se están consiente de los diferentes tipos de amenazas que existen y de los cuales pueden ser víctimas.

Esto conlleva a que usen diversas técnicas de protección contra las amenazas.

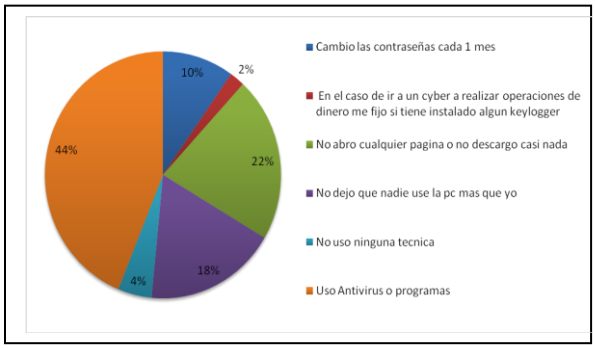

Figura 5. Técnicas que la gente conoce para protegerse de una amenaza

5. Situación actual de la Seguridad Informática del mercado corporativo en el Ecuador

De las encuestas realizadas un porcentaje mayor al cincuenta por ciento corresponde al mercado corporativo, las mismas que superan en más del 50% los 250 empleados catalogándose así como grandes empresas, los sectores que predomina en estas son Comercio y Financiero con un 20 y 22 % respectivamente, con un alcance a nivel nacional de cada una de ellas.

Del grupo de las empresas corporativas tenemos que un 57% abarcan el territorio nacional, entiéndase así que tienen presencia en las principales ciudades del Ecuador, aquí también podemos notar la importancia en la actualidad del Internet para el negocio ya que de este mismo grupo en un 100% tienen contratado servicio de Internet y un 74% usa aplicación usa aplicaciones a través de este medio, además un 83% tiene enlaces de transmisión de datos como medio dedicado de comunicación entre sucursales y

empresas. Este uso masivo del Internet en el mercado corporativo Ecuatoriano nos indica que la Seguridad Informática es una pieza fundamental para el desarrollo de las empresas, ya que sin las mismas serian muy vulnerables.

Esto hace que las mayoría de las empresas del mercado corporativo tengan que cumplir con ciertas normas de seguridad informática ya sea impuestas por entes reguladores de acuerdo a su modelo de negocio o servicio, dentro de las principales normas que cumple el mercado corporativo tenemos a ITIL en su gran mayoría con un 35%, COBIT con un 12 %, PCI-DSS con un 10%, JB 2005-834 con un 4%, especial para el mercado financiero y ISO 27001 con un 4%.

ITIL (del inglés Information Technology Infrastructure Library) es una de las normas que el mercado corporativo indica que mas cumple con un 35%, a nuestro parecer esto se debe a que ITIL independientemente del modelo de negocio da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI, que es si es lo que toda organización busca.

Siguiendo con nuestro análisis de mercado Corporativo tenemos que solo un 24% realiza out-sourcing de seguridad informática a pesar de que solo el 50% tiene posee un área de seguridad informática dentro de la organización, esto indica que no se está poniendo en un primer plano la seguridad informática dentro de ciertas empresas.

El firewall sigue siendo un elemento casi por default dentro de la organizaciones para la protección de la seguridad perimetral con un nivel de presencia de un 96% dentro del mercado corporativo seguidos por los dispositivos IDS e IPS con u 52 y 52% respectivamente, muy atrás quedan los dispositivos WAF con un 4% de presencia, esto es lógico ya que no aplica su uso a todos los modelos de negocios.

En lo concerniente a políticas de Seguridad un 80% indica que tiene definidas políticas globales de seguridad a pesar de que el 98 % está consciente de que existe la posibilidad de perder información, ya sea por robo, algo preocupante es que solo el 39% cree que cuenta con un alto nivel de seguridad informática.

En lo concerniente a las agresiones físicas externas al sistema eléctrico se muestra que existe preocupación por mantener un buen desempeño del mismo, ya que un 70% indica que cuenta con sistemas de alimentación redundante y un 83% indica que cuenta con sistemas de alimentación ininterrumpida, no así con los sistemas de control de acceso físico ya que solo un 52% menciona que cuentan con sistemas que impiden el acceso físico a los recursos a personal no autorizado y un 54% indica que cuenta con mecanismos físicos que impiden el uso de los sistemas de información a mecanismos no autorizados.

En lo que respecta a los servidores de aplicaciones un 41% ha indicado que ha sido víctima de al menos un ataque donde los tres ataques más recurrentes son DoS con un 32%, Modificación de su sitio web con un 27% y Phishing con un 23%, DoS o Ataque de Denegación de Servicio sigue siendo uno de los principales ataques generados por el cibercrimen.

La información sigue siendo el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros, y la medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups, el mercado corporativo nos indica que el 94% realizan copias de seguridad y casi en su totalidad cuentan con procedimiento para realizar dichas copias, el problema ha este buen procedimiento se da a que solo el 69% de estas copias es automatizada, el resto es propensa al error humano, además solo el 59% es guardada en un lugar de acceso restringido, solo el 65% de estas copias son guardadas fuera del lugar de trabajo, y solo el 80% ha probado en restaurar una copias de estas.

Los mecanismos de identificación y autenticación son muy importante dentro de una organización ya que es un modo de asegurar de que los usuarios son quienes dicen que ellos son, que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así, esto el mercado corporativo Ecuatoriano lo está controlando en su mayoría ya que se indica que el 83% cuenta con procedimientos de identificación y el 89% con procedimientos de autenticación.

La mayoría de los ataques físicos generalmente ocurren cuando una persona tiene acceso a las dependencias, los intrusos pueden ser personas ajenas a la organización o bien personal interno como empleados o contratistas. Cuando un intruso es capaz de acceder a un físicamente a un sistema informático, por lo general puede dejarlo fuera de funcionamiento, es por esta razón que los controles de acceso físico deben estar bien definidos por una organización, en nuestro mercado corporativo el 89% de las empresas indican que cuentan con controles de acceso, esto es un alto porcentaje que nos da a conocer la importancia a la protección de los recursos, el 67% nos indica que cuentan con log o ficheros que les indican los accesos autorizados y los intentos de acceso ilícitos, con la finalidad de detectar intrusos, un 63% de estas empresas indican tener separados los recursos a los que pueden acceder los usuarios autorizados una vez que pasaron los filtros de seguridad, esto es una buena práctica en medida de protección a los recursos.

Los datos obtenidos contra el virus son muy favorables para el sector financiero, ya que un 87% indica contar con herramientas de antivirus corporativo, 85% que su antivirus protege los correos electrónicos y las descargas vía web, como buena práctica el 89% indica que actualiza regularmente su

antivirus, esta puede ser una razón para que solo el 69% haya indicado que alguna vez ha experimentado inconvenientes con algún tipo de virus, ya que todos conocemos que con la gran cantidad de virus existente que difícil no ser víctima al menos una vez de ellos, además puede ser una razón más para que solo el 30% indique que el SPAM actualmente es un problema para su organización.

Los planes de seguridad y contingencia son procesos claves dentro del plan de negocio de una organización para la continuidad del mismo, el mercado corporativo ecuatoriano nos indica que en 72% que cuenta con un plan de seguridad y 78% con un plan de contingencia, estos son números favorables para nuestro mercado.

Correo electrónico, hoy en día uno de los pilares principales en las comunicaciones de una organización, y por ello debe de contar con las debidas protecciones de seguridad informática, en nuestro mercado un 83% indica contar son su propio servidor de correos, esto hace que tengan que contar con soluciones de protección del correo, pero solo 76% lo tiene, y entre los principales tipos de protección de utilizan están los antivirus, anti SPAN y mecanismos de encriptación, algo importante de notar es que el 57% de estos han estando en lista negra (RBL)

Acceso a internet, una de las principales causas en problemas de seguridad informática, es difíciles poder controlar en su totalidad el acceso ya que son los usuarios los que deciden que paginas visitar, es por esta razón que las organizaciones crean políticas para que minimicen el acceso a paginas no seguras que puedan atentar contra la seguridad informática de la organización, en nuestro mercado nos indican que un 83% cuenta con políticas definidas para el acceso a internet, y que un 70% han explicado claramente a sus trabajadores de las mismas, además un 78% cuenta con políticas corporativas para el acceso a internet, y las mismas son limitadas por cargos y por usuarios.

Web Site, hoy en día si no están en internet simplemente no existes para el mundo, es por esto que el 80% del nuestro mercado corporativo cuenta con web site empresarial, y debido a que se maneja data sensible solo un 54% ha decidido alojar su web site en una empresa externa, el resto lo maneja localmente en su red, notamos también que hay un porcentaje considerable que no dispone de herramientas que auditen intentos de acceso a externos.

En general tenemos que solo un 52% cree que el área de la seguridad informática se ha fortalecido en los últimos anos, esto es algo que debe ser considerado y analizado ya que como hemos visto anteriormente las amenazas y los diferentes ataques que existen han aumentado y evolucionado considerablemente, entonces podríamos indicar que la seguridad informática en el Ecuador no está siguiendo el ritmo impuestos por todos los actores que atentan contra ella.

6. Productos de Seguridad Informática en el Ecuador

La empresas ecuatorianas dedicadas a la venta de servicios y productos de tecnología, se han dado cuenta que ante el acelerado desarrollo de la tecnología que se da a nivel mundial y ante el aumento del acceso a internet por parte de los usuarios en el ecuador, donde las empresas casi en un 100% tienen contratado servicio de internet con un porcentaje considerable de los empleados con acceso a este medio y donde los portales web para transacciones online están proliferando, ven la necesidad de ofrecer productos de seguridad informática que vayan a la par con este desarrollo, por esta razón muchas empresas ya cuentan con un portafolio de productos de seguridad informática entre sus soluciones para ofrecer a los clientes, además están surgiendo empresas jóvenes dedicadas a ofrecer este tipo de soluciones.

Entre los productos de seguridad informática que podemos encontrar en el Ecuador notamos que predominan las maracas de Cisco, Fortinet y Checkpoint con sus equipos que seguridad y control.

Tabla 1. Productos de seguridad informática que se ofrecen en el Ecuador.

Ítem	Productos
1	Seguridad Perimetral Gestionada
2	Análisis de Tráfico
3	Análisis del Riesgo
4	Test de Penetración
5	Ethical Hacking
6	Informática Forense
7	Diagnostico de Seguridad de los Sistemas
8	Diagnostico de Vulnerabilidades y Riesgos
9	Planeación y Administración de la Seguridad Informática
10	Planeación Estratégica de Sistemas de Información
11	Asesoría Implantación ISO 27001
12	Auditorías de Seguridad de Información
13	Auditoria IT
14	Software de Seguridad Informática
15	Planes para Contingencias y Seguridad de la información
16	Capacitación
17	Seguridad en Redes

7. Oportunidad de Negocio.

Como hemos podido notar a lo largo del desarrollo del documento, el Ecuador no está excluido del desarrollo y avance tecnológico, la globalización hace que cada día la brecha que existía en tecnología entre nuestro país y el resto del mundo sea más estrecha, la Fibra Optica ha hecho que las distancias se acorten a milisegundos, por ende las empresas en el Ecuador como las del resto del mundo han visto que es inevitable no relacionar su negocio con el Internet, cada día este medio entra mas y mas a formar parte del desarrollo diario de miles de negocios, esto es muy favorable pero así mismo acarrea consigo nuevas amenazas no necesariamente provenientes del Ecuador sino de nivel mundial, por lo tanto las precauciones que se deben tomar en lo concerniente a la seguridad informática deben considerar estas amenazas.

El escenario para los emprendedores en el negocio de la seguridad informática es favorable, los segmentos de clientes están definidos, sabemos que cuentan con vulnerabilidades, las amenazas están latentes no descansan, cada día son más sofisticadas, por lo tanto podemos decir que la necesidad existe solo que somos una sociedad que reacciona ante eventualidades, por ende el desafío esta en concientizar y crear una conciencia proactiva en las empresas para que adopten medidas de protección y empiecen a equiparse y adquirir los productos de seguridad informática que logren reducir sus vulnerabilidades.

Además es momento de que las empresas entiendan que es importante invertir en seguridad informática para resguardar y garantizar la integridad de la información de la compañía, que se considere a la seguridad informática como un activo muy importante, ya que un buen sistema de protección de datos trae mejores resultados en producción, mejora la gestión de sus trabajadores y otorga mayor calidad al negocio.

Vemos que hoy en día las grandes empresas corporativas están ya pensando e invirtiendo en movilidad, en virtualización, en computación en la nube, entonces eso abre un nicho de mercado por explotar en lo concerniente a seguridad informática, esto es algo que ya se está dando y no es algo que puede pasar, por lo tanto la protección de Internet en la nube, de email en la nube y de endpoints en la nube se vuelve inevitable, entonces esta es una buena oportunidad para empezar un negocio ya que la computación en la nube, movilidad, virtualización, mejora la productividad de las empresas y la gran mayoría optaran por contar con estos productos y como ya hemos dicho contar con un buen sistemas de seguridad informática no será una opción sino una obligación para estas empresas.

Los Pymes hoy en día se han constituido en una fuerza de producción importante para el Ecuador, pero su poco presupuesto ha sido un factor importante para no implementar las correctas medidas de seguridad informática para aquellas que quieren protegerse, es por esta razón que surge la necesidad de crear servicios de seguridad gestionada que sean capaces de cubrir las necesidades de seguridad de los Pymes sin que tengan que incurrir en grandes gastos de entrada ya sea en adquisición de equipos, personal, implementación, etc.

8. Conclusiones.

De los resultados obtenidos por las encuestas podemos concluir de manera general lo siguiente:

1. a La seguridad informática en el Ecuador aun no alcanza un nivel de madurez que garantice y de confianza a los actores del negocio sobre el resguardo de la información la cual hoy en día constituye uno de los activos más importantes en las organizaciones y cada día con el avance tecnológico y la penetración del internet en el país están más expuesta a ser víctima del cibercrimen.
2. El mercado corporativo sigue marcando la diferencia en lo concerniente a tecnología pero seguido muy de cerca de los Pymes, ambos tienen un porcentaje de uso del internet de un 100%, esto indica que el riesgo de ser víctimas del cibercrimen mundial ha aumentado ya que cuentan con la conexión al mundo globalizado.
3. El uso de aplicaciones a través de internet por parte de los usuarios que forman parte de una empresa en la actualidad es de un alto porcentaje 77%, ante este porcentaje si no se cuenta con las debidas protecciones de seguridad informática podría acarrear un problema grave a la seguridad de la información de las empresas.
4. El servidor de correos hoy en día es una de los dispositivos de aplicaciones consideramos como mas importantes por las empresas para el desenvolvimiento diario, seguido por el dispositivo de base de datos y el servidor de dominios, de aquí podemos decir que el hecho de que el correo se haya convertido en una herramienta muy valiosa para una empresa debe ser considera en los planes de seguridad informática tanto para su integridad y disponibilidad ya que el uso masivo de este medio por los usuarios hace que en muchos casos se dependa del uso de las buenas prácticas que los mismos apliquen, no obstante las empresas no deben esperar que esto se dé por parte de los usuarios, y deben implementar medidas de seguridad informática que garanticen la integridad y disponibilidad del correo.
5. En el Ecuador se sigue considerando que el mantener el buen desempeño de los dispositivos que permiten el flujo de datos en la red es suficiente para garantizar un buen desenvolvimiento de las actividades diarias de la empresa, dejando así en otro plano a la seguridad informática.
6. Los dispositivos de seguridad perimetral más usados o aplicados son Firewall IDS e IPS

respectivamente, esto ha prevalecido durante ya algún tiempo.

7. Las Empresas Ecuatorianas aun creen que no deben mantener un área dentro de la misma con personal especializado, es tanto así que en el sector financiero podemos encontrar en mayor porcentaje solo una persona a cargo de la seguridad informática, es por esta razón que a nivel ejecutivo no está contemplado un presupuesto la asignación de un presupuesto para el área de seguridad informática.

8. La encuesta para este documento fue realizada al personal técnico involucrado directamente con el mantenimiento de la red, estas personas en un alto porcentaje indicaron estar consientes de que no poseen un alto nivel de seguridad de la información, esto nos da a conocer que el problema para la no asignación los suficientes recursos a la seguridad informática esta en mayor parte del lado ejecutivo de la empresa, a pesar de esto se están comenzando a implementar políticas se seguridad informática que contribuyan a mantener la confidencialidad, integridad y disponibilidad de la información.

9. Las empresas Ecuatorianas si se han preocupado en mantener un sistemas de protección eléctrica de alta disponibilidad e ininterrumpidas, pero no así con los sistemas de control de acceso físico a los recursos, ya que la mayoría no cuenta con ellos, ni con mecanismos físicos que impidan el uso de los sistemas de información a mecanismos no autorizados.

10. El mantener copias de seguridad de la información es algo que las empresas en su mayoría lo practicas, esto es una buena práctica ya que le garantiza ante alguna perdida de información ya sea por robo o desastre poder contar con el respaldo de la ultima copia, el problema que notamos en este proceso es que un porcentaje considerable de empresas no cuenta con un procedimiento automatizado para la obtención de las copias de seguridad haciendo que estén propensas al error humano, también no cuentan con un lugar de acceso restringido para el almacenamiento y un lugar externo fuera de las oficinas para el mismo.

11. Las empresas han llegado a comprender la importancia de los mecanismos de identificación y autenticación ya que esto les garantiza que solo los usuarios autorizados puedan hacer uso de los sistemas de la empresa, es por esto que notamos que un alto porcentaje cuenta con estas políticas de buenas prácticas dentro de las empresas Ecuatoriana, de igual manera a estos controles se suman los controles de acceso físico.

12. Las estadísticas nos indican que en Ecuador ITIL, es el estándar y las buenas prácticas que están en las áreas de la seguridad de la información en los departamentos de tecnología, eso de sebe a que ITIL independientemente del modelo de negocio ayuda a las organizaciones a lograr la calidad y eficiencia en las operaciones de TI.

13. El virus, el desafío de todos los sistemas de seguridad informática, el cual paso de ser el juego de un hacker a convertirse en el principal arma del cibercrimen, actualmente las empresas ecuatorianas han tomado medidas contra este mal, lamentablemente no siempre las medidas que se toman son las más adecuadas.

14. Hoy en día es conocido a nivel global que el cifrado en las comunicaciones es un buen método ante el robo de información, sin embargo esta no es una práctica que menos del 50% de las empresas en el ecuador la práctica, al parecer se conoce de su uso pero no se hace conciencia de su importancia.

15. Es notorio decir que el poco entendimiento de la seguridad informática y la falta de apoyo que se le da a la misma por parte de los directivos, no puede ser escusa para no avanzar en un sistema de gestión de seguridad, conocemos que la inversión en seguridad es costosa pero los daños materiales que puede causar la inseguridad puede ser mucho mayor.

16.- En el Ecuador, como en el resto del mundo, hemos notado que la movilidad es inevitable para expandir los servicios y mejorar el negocio, apesar de esto nadie de los encuestados ha hecho énfasis sobre la seguridad informática en los dispositivos móviles.

9. Recomendaciones.

1. Como ya lo hemos mencionado antes, los nuevos emprendedores en el negocio de la seguridad informática tienen como desafío hacer que las empresas comiencen a entender la importancia de la seguridad informática, deben trabajar para que esta área tenga más apoyo del ejecutivo de la empresa

2. La capacitación dentro de las empresas en seguridad informática tiene que convertirse en el primer paso para el entendimiento de la importancia de la misma, esta es una oportunidad de negocio que va de acorde a las tendencias actuales y futuras

3. La seguridad informática gestionada se convertirá en la primer alternativa para las pequeñas empresas por ende hay que poner gran atención es esta oportunidad de negocio

4. Algo que no se ha mencionado en este documento, es que el Ecuador no cuenta con un organismo de control, monitoreo y regulación de la seguridad informática, esta es algo que se hace emergente implementar a corto plazo, ya que ayudara en el fortalecimiento de la seguridad informática en país y por ende la empresas se podrán apoyar en este organismo

5. Ya es hora de pensar en forma globalizada y dejar de creer que el cibercrimen o ciberterrorismo no puede pasas aquí en este país, una vez más repetimos que los problemas de seguridad informática son globalizados y por ende las medidas de protección que debemos tomar deben ser de igual magnitud

6. La penetración del internet en el mercado HOME está en aumento, las redes sociales crecen junto con sus usuarios que cada vez proporcionan más datos personales, en contraparte las ingeniería social lo hace de igual manera, por lo tanto la protección en nuestros hogares no es una opción, todos los miembros del hogar usen un computador con acceso internet deben contar con el conocimiento necesario en protección y navegar a la defensiva

10. Agradecimientos

A todos aquellos que de alguna u otra manera y de forma incondicional nos han ayudado a alcanzar este logro, un logro que ha cambiado nuestras vidas de forma positiva y nos encamina hacia nuevas metas.

11. Referencias

[1] Wikipedia, definición de Amenazas en Seguridad Informática,
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta, noviembre 2010

[2] Wikipedia, tipos de Amenazas en Seguridad Informática,
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta, noviembre 2010

[3] Redalyc, codificación de la Información,
http://redalyc.uaemex.mx/pdf/903/90312176007.pdf, fecha de consulta, noviembre 2010

[4] Segu Info, tipos de Cortafuegos, http://www.seguinfo.com.ar/firewall/firewall.htm, fecha de consulta noviembre 2010

[5] Panda Security, Informe Trimestral PandaLabs, segundo trimestre 2010,
http://www.pandasecurity.com/img/enc/Informe_Trimestral_PandaLabs_T2_2010.pdf, fecha de consulta Febrero 2011

[6] Panda Security, Caso Mariposa,
http://www.pandasecurity.com/spain/enterprise/media/pressreleases/
viewnews?noticia=10084, fecha de consulta Marzo 2011

[7] Panda Security, Cloud Protection,
http://cloudprotection.pandasecurity.com/index.php?lang=es, fecha de consulta
Marzo 2011